

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Shinichi KAWAMURA

SERIAL NO: New Application

GAU: Unassigned

FILED: Herewith

EXAMINER: Unassigned

FOR: MODULAR ARITHMETIC APPARATUS AND METHOD HAVING HIGH-SPEED BASE CONVERSION
FUNCTION

INFORMATION DISCLOSURE STATEMENT UNDER 37 CFR 1.97

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

Applicant(s) wish to disclose the following information.

REFERENCES

- ☒ The applicant(s) wish to make of record the references listed on the attached form PTO-1449. Copies of the listed references were cited or provided in parent application serial no. 09/699,481 filed October 31, 2000, as were either statements of relevancy or any readily available English translations of pertinent portions of any non-English language references
- ☐ A check is attached in the amount required under 37 CFR §1.17(p).

RELATED CASES

- ☐ Attached is a list of applicant's pending application(s) or issued patent(s) which may be related to the present application. A copy of the patent(s), together with a copy of the claims and drawings of the pending application(s) is attached along with PTO 1449.
- ☐ A check is attached in the amount required under 37 CFR §1.17(p).

CERTIFICATION

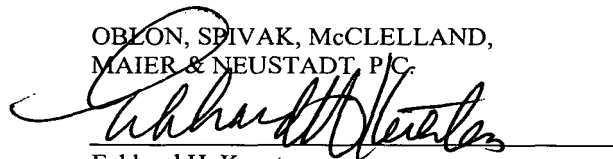
- ☐ Each item of information contained in this information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this statement.
- ☐ No item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application or, to the knowledge of the undersigned, having made reasonable inquiry, was known to any individual designated in 37 CFR §1.56(c) more than three months prior to the filing of this statement.

DEPOSIT ACCOUNT

- ☒ Please charge any additional fees for the papers being filed herewith and for which no check is enclosed herewith, or credit any overpayment to deposit account number 15-0030. A duplicate copy of this sheet is enclosed.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Eckhard H. Kuesters

Registration No. 28,870



22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

Michael E. Monaco
Registration No. 52,041

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Shinichi KAWAMURA

SERIAL NO: New Application

GAU: Unassigned

FILED: Herewith

EXAMINER: Unassigned

FOR: MODULAR ARITHMETIC APPARATUS AND METHOD HAVING HIGH-SPEED BASE CONVERSION
FUNCTION

INFORMATION DISCLOSURE STATEMENT UNDER 37 CFR 1.97

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

Applicant(s) wish to disclose the following information.

REFERENCES

- ☒ The applicant(s) wish to make of record the references listed on the attached form PTO-1449. Copies of the listed references were cited or provided in parent application serial no. 09/699,481 filed October 31, 2000, as were either statements of relevancy or any readily available English translations of pertinent portions of any non-English language references
- ☐ A check is attached in the amount required under 37 CFR §1.17(p).

RELATED CASES

- ☐ Attached is a list of applicant's pending application(s) or issued patent(s) which may be related to the present application. A copy of the patent(s), together with a copy of the claims and drawings of the pending application(s) is attached along with PTO 1449.
- ☐ A check is attached in the amount required under 37 CFR §1.17(p).

CERTIFICATION

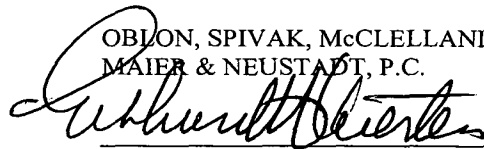
- ☐ Each item of information contained in this information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this statement.
- ☐ No item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application or, to the knowledge of the undersigned, having made reasonable inquiry, was known to any individual designated in 37 CFR §1.56(c) more than three months prior to the filing of this statement.

DEPOSIT ACCOUNT

- ☒ Please charge any additional fees for the papers being filed herewith and for which no check is enclosed herewith, or credit any overpayment to deposit account number 15-0030. A duplicate copy of this sheet is enclosed.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Eckhard H. Kuesters

Registration No. 28,870



22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

Michael E. Monaco
Registration No. 52,041

Form PTO 1449 (Modified)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTY DOCKET NO. 240527US2SRD DIV		SERIAL NO. New Application	
LIST OF REFERENCES CITED BY APPLICANT				APPLICANT Shinichi KAWAMURA			
				FILING DATE Herewith		GROUP Unassigned	
U.S. PATENT DOCUMENTS							
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUB CLASS	FILING DATE IF APPROPRIATE
	AA	4,996,527	02/91	Houk et al			
	AB	5,050,120	9/91	Houk, Theodore L.			
	AC	5,107,451	4/92	Houk, Theodore L.			
	AD	5,987,487	11/99	Welland, David R.			
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						
	AL						
	AM						
	AN						
FOREIGN PATENT DOCUMENTS							
		DOCUMENT NUMBER	DATE	COUNTRY	TRANSLATION YES NO		
	AO						
	AP						
	AQ						
	AR						
	AS						
	AT						
	AU						
OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, etc.)							
	AV	Shinichi KAWAMURA, et al., "COX-ROWER ARCHITECTURE FOR FAST PARALLEL MONTGOMERY MULTIPLICATION," Lecture Notes in Computer Science, No. 1807, May 2000, pgs. 523-538					
	AW	Karl C. POSCH, et al., "MODULO REDUCTION IN RESIDUE NUMBER SYSTEMS," IEEE Transactions on Parallel and Distributed Systems, Vol. 6, No. 5, May 1995, pgs 449-454					
	AX	J. SCHWEMMEIN, et al., "RNS-MODULO REDUCTION UPON A RESTRICTED BASE VALUE SET AND ITS APPLICABILITY TO RSA CRYPTOGRAPHY," Computers and Security, Vol. 17, No. 7, 1998, pgs. 637-650					
	AY	Jean-Claude BAJARD, et al., "AN RNS MONTGOMERY MODULAR MULTIPLICATION ALGORITHM," IEEE Trans. On Computers, Vol. 47, No. 7, pgs, 1998, 766-776					
	AZ	Pascal PAILLIER, "LOW-COST DOUBLE-SIZE MODULAR EXPONENTIATION OR HOW TO STRETCH YOUR CRYPTOPROCESSOR," Lecture Notes in Computer Science, No. 1560, 1999, pgs. 223-234					
					<input type="checkbox"/> Additional References sheet(s) attached		
Examiner					Date Considered		
*Examiner: Initial if reference is considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.							